Amendments to the Specification:

Please insert the following on page 1, line 3:

Cross-reference to related applications.

This application is a 35 U.S.C. 371 of PCT application PCT/FR00/00190 filed January 27, 2000.

Field of the invention

Please insert the following on page 1, line 6:

Background of the invention

Please amend page 1, line 24 as follows:

~~**Method**~~ **Brief summary of the invention**

Please insert the following on page 3, lines 19:

Referring now to Figure 1, an operation flow for a process 100 is shown. The process 100 begins at operation 105 and proceeds to operation 110 in which private Q_1 Q_2 ... Q_m and public value G_1, G_2 ... G_m are obtained, where m is greater than 1. The process then proceeds to operation 115 in which the private values Q_1, Q_2 ... Q_m are used in an authentication method or a signature method. The process ends at operation 120.

Please insert the following on page 4, line 17:

Detailed description of the invention.

Please replace the paragraph beginning on page 4, line 17 with the following amended paragraph:

Case of the proof of the authenticity of an entity

In a first alternative embodiment, the method according to the invention is designed to prove the authenticity of an entity known as a demonstrator to an entity known as the controller. Said demonstrator entity comprises the witness. Said demonstrator and controller entities execute the following steps[[:]] as shown in the flow chart or process 200 in Figure 2.

The process 200 begins at operation 205 and proceeds to operation 210 in which occurs:

- **Step 1: act of commitment R**

At each call, the witness computes each commitment **R** by applying the process specified here above. The demonstrator sends the controller all or part of each commitment **R**.

The process 200 then proceeds to operations 215 and 220 in which occurs:

- **Step 2: act of challenge d**

The controller, after having received all or part of each commitment **R,** produces challenges **d** whose number is equal to the number of commitments **R** and sends the challenges **d** to the demonstrator.

The process 200 then proceeds to operation 225 in which occurs:

- **Step 3: act of response D**

The witness computes the responses **D** from the challenges **d** by applying the above-specified process.

The process 200 then proceeds to operation 230 in which occurs:

- **Step 4: act of checking**

The demonstrator sends each response **D** to the controller.

The process ends at operation 235.

Please replace the paragraph beginning on page 5, line 24 with the following amended paragraph:

Case of the proof of the integrity of the message

In a second alternative embodiment capable of being combined with a first one, the method of the invention is designed to provide proof to an entity, known as the controller entity, of the integrity of a message **M** associated with an entity called a demonstrator entity. Said demonstrator entity comprises the witness. Said demonstrator and controller entities perform the following steps [[:]] as shown in the flow chart of process 300 in Figure 3.

The process 300 begins at operation 305 and proceeds to operation 310 in which occurs:

- **Step 1: act of commitment R**

At each call, the witness computes each commitment **R** by applying the process specified here above.

The process 300 then proceeds to operations 315 and 320 in which occurs:

- **Step 2: act of challenge d**

The demonstrator applies a hashing function **h** whose arguments are the message **M** and all or part of each commitment **R** to compute at least one token **T**. The demonstrator sends the

token **T** to the controller. The controller, after having received a token **T**, produces challenges **d** equal in number to the number of commitments **R** and sends the challenges **d** to the demonstrator.

The process 300 then proceeds to operation 325 in which occurs:

- **Step 3: act of response D**

The witness computes the response **D** from the challenges **d** by applying the above-specified process.

The process 300 then proceeds to operation 330 in which occurs:

- **Step 4: act of checking**

The demonstrator sends each response **D** to the controller. The controller, having the **m** public values $G_1, G_2, ..., G_m$, computes a reconstructed commitment **R'**, from each challenge **d** and each response **D**, this reconstructed commitment **R'** satisfying a relationship of the type

$$R' = G_1^{d1} . G_2^{d2} . G_m^{dm} . D^v \bmod n$$

or a relationship of the type

$$R' = D^v / G_1^{d1} . G_2^{d2} . ... G_m^{dm} . \bmod n$$

Then the controller applies the hashing function **h** whose arguments are the message **M** and all or part of each reconstructed commitment **R'** to reconstruct the token **T'**. Then the controller ascertains that the token **T'** is identical to the token **T** transmitted.

The process ends at operation 335.

Please insert the following on page 43, line 23:

Referring now to Figure 4, a process 400 is shown. The process 400 begins at operation 405 and proceeds to operation 410 in which integers are randomly chosen. The process 400 then proceeds to operation 415 in which commitments are computed. Tokens are computed in operation 420 and bits of the tokens are identified in operation 425. The process 400 then proceeds to operation 430 in which a response is computed. The process ends at operation 435.

Please insert the following on page 45, line 14:

Referring now to Figure 5, the above noted methods can be implemented on a system 500 including a memory 505 storing instructions 520 which are executed on a processor 510.